IN THE UNITED STATES DISTRICT COURT FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA

Plaintiff

CRIMINAL No. 12-29/

:

(Judge CMNBY

MONEYGRAM INTERNATIONAL, INC.

v.

•

Defendant

<u>INFORMATION</u>

FILED HARRISBURG

The United States informs the Court that:

BACKGROUND

NOV 9 - 2012

MARY E. D'ANDREA, CLERK Per

At all times relevant to this Information:

Relevant Entities

- 1. The defendant, MONEYGRAM INTERNATIONAL, INC. ("MONEYGRAM"), was a publicly traded, global money services business ("MSB"), incorporated under the laws of Delaware, and headquartered in or around Minneapolis, Minnesota, and later in or around Dallas, Texas. MONEYGRAM provided a service that enabled customers to transfer money to various locations in the United States and around the world. MONEYGRAM operated worldwide through a network of up to 275,000 locations in 190 countries.
- 2. "MoneyGram Outlets" or "Outlets" were independently owned entities that were contractually authorized to transfer money through MONEYGRAM's money transfer system.

 Typically, MoneyGram Outlets were businesses that primarily provided other types of goods and

services, and also offered money transfers through MONEYGRAM.

- 3. "MoneyGram Agents" or "Agents" were individuals or entities that owned and/or operated MoneyGram Outlets. MoneyGram Agents received a commission from MONEYGRAM on transactions processed at their Outlets. MONEYGRAM Agents are independent contractors, not MONEYGRAM employees. MONEYGRAM had the legal right to terminate Agents for a variety of reasons, including suspected involvement in fraud.
- 4. "Perpetrators" were individuals that created schemes to defraud the public using MONEYGRAM's money transfer system ("the scheme to defraud"). These Perpetrators included, among other people, certain MoneyGram Agents.
- 5. The "MoneyGram Call Center" or "Call Center" was located in or around Lakewood, Colorado. Among other responsibilities, the Call Center fielded complaints of MoneyGram customers from around the world who reported they were the victims of fraud. These complaints, known as "Consumer Fraud Reports," were typically filed by the customer within a few days of the fraudulent transaction. The Consumer Fraud Report listed the name and address of the customer allegedly victimized, the send amount, the date of the transfer, the intended recipient, and a description from the customer of how they believe they were defrauded. The Call Center then forwarded the Consumer Fraud Report data to MONEYGRAM's Fraud Department for investigation.

Money Transmitting Process

6. To send money using MONEYGRAM's money transfer system, customers went to a MoneyGram Outlet and completed a "send" form designating the name of the recipient and the state or province and country where the money was to be sent. The MoneyGram Agent was required to enter the information from the send form along with the transfer amount into a

transaction database established and maintained by MONEYGRAM as part of its central electronic network in or around Minneapolis, Minnesota. MONEYGRAM charged a fee based on the transfer amount and the destination location. Customers then gave the MoneyGram Agent cash to cover the transfer amount and the MoneyGram fee. Customers were given an eight-digit MoneyGram reference number for the transaction.

- 7. To receive a money transfer, MONEYGRAM required the payee to physically appear at a MoneyGram Outlet and complete a handwritten application known as a "receive" form. On the receive form, MONEYGRAM required the payee to list his or her name, address and telephone number; the name, city, state or province of the sender; and the expected transfer amount. The MoneyGram Agent would then query MONEYGRAM's transaction database to find the money transfer intended for the payee. For all money transfers in amounts equal to or greater than \$900, MONEYGRAM required the payee to present a valid identification document for examination by the MoneyGram Agent. MONEYGRAM then required the MoneyGram Agent to enter the payee's name, address, telephone number, and identification document serial number into its transaction database. Depending on the MoneyGram Outlet, the payee would receive the transfer in cash or in the form of a MoneyGram transfer check or money order.
- 8. Money transferred between two individuals using MONEYGRAM's transfer system was never physically transported from the sender to the receiver. Rather, the details from the send transaction were recorded in MONEYGRAM's transaction database. The sending Agent was then responsible for depositing the cash it received from the customer into its bank account by the next business day. MONEYGRAM then removed the transfer amount plus the MoneyGram fee from the Agent's bank account typically on the second business day after the transaction. Even though the customer's money did not reach MONEYGRAM's account for at least two business

days, MONEYGRAM made the funds available to the payee as soon as ten minutes after the initial transaction based on the information it had in its transaction database. Depending on the contractual agreement between the payout Agent and MONEYGRAM, the Agent would pay the payee with cash on hand or issue the payee a MoneyGram transfer check or money order.

MONEYGRAM would then add money to the payout Agent's bank account for the money paid to the payee. At all times before the payee received cash from the MoneyGram Agent or cashed the MoneyGram transfer check, MONEYGRAM had the ability to refuse to conduct a transaction, reverse a transaction, or stop payment on the MoneyGram transfer check at its discretion.

THE SCHEME TO DEFRAUD

The Scheme to Defraud Operated through MONEYGRAM's Money Transfer System

- 9. From as early as 2003, and continuing through 2009, MONEYGRAM, through the Consumer Fraud Reports and other data its Fraud Department collected, knew that specific MoneyGram Agents were involved in a scheme to defraud that relied on a variety of false promises and other representations to the public in order to trick unsuspecting victims into sending money through participating MoneyGram Agents and MoneyGram Outlets. The victims' money would then be taken by the Perpetrators and none of the false promises or representations were fulfilled. Specifically, victims were contacted by phone, U.S. mail, interstate courier, or the Internet, and were fraudulently induced to send money to the Perpetrators. The fraud was committed by, among other things:
 - Falsely promising victims they would receive large cash prizes, lottery winnings, fictitious loans, or other payments;
 - b. Falsely offering various high-ticket items for sale over the Internet at deeply discounted prices;

- c. Falsely promising employment opportunities as "secret shoppers" who would be paid to evaluate retail stores; or
- d. Placing a distressed phone call falsely posing as the victim's relative and claiming to be in trouble and in urgent need of money.
- 10. The Perpetrators then falsely represented that in order to receive the thing they were promised, the victims needed to give them some money in advance. For example, in situations where the victims were promised cash prizes or lottery winnings, the victims were told they had to pay taxes, customs' duties, or processing fees up front. The victims were then directed to send the advance payment to fictitious payees using MONEYGRAM's money transfer system.
- 11. After the victims completed the money transfer, they were instructed to contact the Perpetrators to give them the MoneyGram reference number for the transaction. The Perpetrators then brought the victims' MoneyGram reference number to participating MoneyGram Agents to remove the victims' money from the MoneyGram transfer system.
- 12. The MoneyGram Agents knowingly entered false addresses, telephone numbers, and personal identification document information for these transactions into the MoneyGram database. In doing so, the MoneyGram Agents concealed the true identities of the Perpetrators, as well as their ownership and control of the fraudulently obtained funds. The MoneyGram Agents then gave the Perpetrators the victims' money, after subtracting their own fees for completing the fraudulent transaction.
- 13. At no time were the victims provided with what they were falsely promised by the Perpetrators.

MONEYGRAM Knew Its Agents Were Involved in the Scheme to Defraud

- 14. From in or about 2004 through 2009, MoneyGram customers filed approximately 63,814 Consumer Fraud Reports involving transfers paid out at MoneyGram Outlets in the United States and Canada totaling approximately \$128,445,411 in losses to victims. The victims who generated the vast majority of these Consumer Fraud Reports described losing money through the scheme outlined above. The total scope of the fraud scheme, however, was more expansive because not every victim of the fraud scheme reported the fraud to MoneyGram.
- 15. As early as 2003, MONEYGRAM's Fraud Department compiled the Consumer Fraud Report data in an electronic fraud database that detailed the number of fraud complaints for each MoneyGram Agent. Within MONEYGRAM, the Fraud Department recommended to senior management that numerous specific MoneyGram Agents and Outlets be terminated for fraud due to the high number of Consumer Fraud Reports generated.
- 16. Despite these recommendations, MONEYGRAM's former senior management refused to allow its Fraud Department to terminate an Agent or close an Outlet for fraud without approval from executives on the sales side of the business. As a result, the Fraud Department's termination recommendations were rarely accepted. For example, in or about March 2007, the Fraud Department after receiving a Civil Investigative Demand from the Federal Trade Commission regarding consumer fraud in Canada recommended that MONEYGRAM immediately close 32 specific MoneyGram Outlets in Canada that had high levels of reported fraud. In or about April 2007, a meeting was held to discuss the closure of these Outlets. In attendance at the meeting were MoneyGram officers at the senior and executive vice-president level. Ultimately, these officers rejected the Fraud Department's recommendation and none of the 32 Outlets were closed. Following this meeting, MONEYGRAM continued to receive complaints

from its customers indicating these MoneyGram Outlets were still involved in fraud. Nevertheless, MONEYGRAM continued to process transactions from the Outlets that they knew were involved in fraud.

MONEYGRAM also knew that certain Agents with high levels of reported fraud were making MoneyGram transfer checks from fraudulent transactions payable to third parties, who were depositing the checks into a single bank account, instead of to the purported payee. This practice, known as "check pooling," allowed the Perpetrators to collect MoneyGram transfer checks at multiple Outlets, deposit those checks in a manner that concealed the identity of the Perpetrators, who were the true recipients of the funds, and then ultimately withdraw and distribute the proceeds among the Perpetrators.

MONEYGRAM Assisted and Profited from the Scheme to Defraud

- 18. Despite its knowing that specific MoneyGram Agents were involved in the scheme to defraud, MONEYGRAM continued to process fraudulent transactions through these Agents.

 MONEYGRAM's processing of these fraudulent transactions was critical to the success of the scheme to defraud because the Perpetrators relied on MONEYGRAM's money transfer system to receive the victims' money.
- 19. MONEYGRAM's Fraud Department attempted to implement policies that would have required the termination of a MoneyGram Agent or Outlet if the Agent or Outlet had a certain number of Consumer Fraud Reports. These policies were repeatedly rejected by the sales side of the business. For example, in or about March 2007, MONEYGRAM's Fraud Department recommended that MONEYGRAM terminate any Agent or Outlet that had 15 Consumer Fraud Reports in three months, 20 Consumer Fraud Reports in six months, or 40 Consumer Fraud Reports in one year. This policy was never approved by sales and therefore never implemented.

- 20. Subsequently, in or about November 2008, sales finally approved a termination policy. Under the approved policy, MONEYGRAM would terminate any Agent that had Consumer Fraud Reports greater than one percent of all MONEYGRAM's Consumer Fraud Reports worldwide. In 2008, there were approximately 27,000 Consumer Fraud Reports filed worldwide. Thus, at a minimum, MONEYGRAM's new policy meant an Agent would not be terminated for fraud unless the Agent incurred at least 270 Consumer Fraud Reports in one year nearly seven times as many Consumer Fraud Reports as under the previous policy. Even this weaker policy was never consistently enforced prior to April 2009.
- 21. As a result of MONEYGRAM's failure to implement and enforce a termination policy, MoneyGram Agents complicit in the scheme to defraud were permitted to stay open for longer periods of time and the fraudulent activity skyrocketed. In 2004, victimized MoneyGram customers in the United States and Canada filed approximately 1,575 Consumer Fraud Reports. For 2008, that number jumped over ten fold, to approximately 19,614 reported frauds.
- by increasing the number of transactions these Agents could process each day, granting these Agents additional MoneyGram outlets from which to operate, and increasing their compensation. For example, by in or about June 2005, James Ugoh, a MoneyGram Agent who generated substantial revenues for MONEYGRAM, owned or operated four MoneyGram Outlets in or around Toronto, Canada. By this time, Ugoh's Outlets had nearly 100 Consumer Fraud Reports totaling approximately \$350,000 in losses to victims. MONEYGRAM did not terminate its relationship with Ugoh. Instead, on or about June 18, 2005, MONEYGRAM threw a party in Ugoh's honor. Over the next four years, MONEYGRAM allowed Ugoh to open eight additional MoneyGram Outlets, gave Ugoh a substantial bonus, and dramatically increased Ugoh's

commissions. MONEYGRAM did not terminate its relationship with Ugoh until in or about February 2009, when Canadian law enforcement officers executed search and arrest warrants at a number of MoneyGram Outlets in or around Toronto. By that time, Ugoh's outlets had approximately 1,733 Consumer Fraud Reports totaling approximately \$3.3 million in reported losses to victims who had used MONEYGRAM's services.

23. MONEYGRAM profited from the fraud schemes by, among other ways, collecting fees and other revenues on each fraudulent transaction initiated by the Perpetrators including MoneyGram Agents.

COUNT ONE (Wire Fraud, Aiding and Abetting) (18 U.S.C. §§ 1343 and 2)

- 24. The allegations set forth in paragraphs 1 through 23 of this Information are hereby re-alleged as if fully set forth herein.
- 25. Between January 2004 and August 2009, in the Middle District of Pennsylvania and elsewhere, the defendant,

MONEYGRAM

and others known and unknown, knowingly devised and intended to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations and promises, and for the purpose of executing the scheme to defraud did transmit, and did aid, abet, counsel, command, induce, procure, and cause to be transmitted, by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, to wit, MONEYGRAM processed thousands of wire communications, totaling at least \$100,000,000, including the following:

Count	Date	MONEYGRAM Wire Communication		Receive Agent	Transfer Amount	Reference Number
		From	To (in or around)	Location		
1	5/29/2008	Victim-1 Palmyra, PA	Minneapolis, MN	James Ugoh Toronto, Canada	\$1,000	98240944

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT TWO

(Willful Failure to Maintain an Effective Anti-Money Laundering Program) (31 U.S.C. §§ 5318(h), 5322)

- 26. The allegations set forth in paragraphs 1 through 23 of this Information are hereby re-alleged as if fully set forth herein.
- 27. Title 31, United States Code, Sections 5311 through 5330 (the "Bank Secrecy Act"), and the regulations promulgated there under (collectively, the "Bank Secrecy Laws"), required every domestic financial institution to maintain appropriate procedures to ensure compliance with the Bank Secrecy Laws and to guard against money laundering.
- 28. MONEYGRAM was a domestic financial institution, and more specifically, a money services business, as defined in the Bank Secrecy Laws.
- 29. From in or about 2004, and continuing until in or about 2009, in the Middle District of Pennsylvania and elsewhere, defendant,

MONEYGRAM

a domestic financial institution and money services business, did willfully violate the Bank Secrecy Act, Title 31, United States Code, Section 5318(h), and regulations issued there under, to wit, Title 31, Code of Federal Regulations, Section 1022.210(a) (formerly Section 103.125(a)), by failing to develop, implement, and maintain an effective anti-money laundering program, while violating another law of the United States, to wit, Title 18, United States Code, Sections 1343 (Wire Fraud) and 2 (Aiding and Abetting) and as part of a pattern of any illegal activity involving more than \$100,000 in a 12-month period.

- 30. Specifically, MONEYGRAM willfully failed to implement and maintain effective policies, procedures, and internal controls including, among others:
 - (1) failure to implement policies and procedures governing the termination of

- Agents involved in fraud and money laundering;
- (2) filing of Suspicious Activity Reports ("SARs"), in which MONEYGRAM incorrectly listed the victim of fraud as the individual who was the likely wrongdoer and failing to file SARs on their Agents who MONEYGRAM knew were involved in the fraud;
- (3) failure to implement policies or procedures to file the required SARs when victims reported fraud to MONEYGRAM on transactions over \$2,000;
- (4) failure to sufficiently resource and staff its anti-money laundering program;
- (5) failure to conduct effective anti-money laundering audits of its Agents;
- (6) failure to implement policies or procedures to review MoneyGram transfer checks of Agents known or suspected to be involved in "check pooling";
- (7) failure to conduct adequate due diligence on prospective MoneyGram

 Agents; and
- (8) failure to conduct adequate due diligence on MoneyGram Agents seeking additional MoneyGram Outlets.

All in violation of Title 31, United States Code, Sections 5318(h) and 5322(b) and Title 31, Code of Federal Regulations, Section 1022.210(a) (formerly Section 103.125(a)).

FORFEITURE ALLEGATIONS

31. As a result of committing wire fraud in Count One of this Information, the defendant, MONEYGRAM INTERNATIONAL, INC., shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461, any and all property, real and personal, constituting and derived from proceeds obtained directly and indirectly as a result of the said offenses, including, but not limited to, at least \$100,000,000, a sum of money representing an approximate amount of proceeds obtained as a result of the said offenses.

SUBSTITUTE ASSET PROVISION

- 32. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:
 - a. cannot be located upon the exercise of due diligence;
 - b. has been transferred or sold to, or deposited with, a third party;
 - c. has been placed beyond the jurisdiction of the Court;
 - d. has been substantially diminished in value; or
 - e. has been commingled with other property which cannot be subdivided without difficulty,

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981; Title 21, United States Code, Section 853; and Title 28, United States Code, Section 2461.)

United States Attorney
Middle District of Pennsylvania

JAIKUMAR RAMASWAMY
Chief, Asset Forfeiture and
Money Laundering Section
Criminal Division
United States Department of Justice